Proceedings of the Informing Science + Information Technology Education Conference

An Official Publication of the Informing Science Institute
InformingScience.org

InformingScience.org/Publications

July 31 - August 5 2017, Ho Chi Minh City (Saigon), Vietnam

REVIEW OF BEHAVIOURAL THEORIES IN SECURITY COMPLIANCE AND RESEARCH CHALLENGES

Hiep-Cong Pham*	RMIT University Vietnam, Ho Chi Minh City, Vietnam	hiep.pham@rmit.edu.vn
Linda Brennan	RMIT University, Melbourne, Australia	linda.brennan@rmit.edu.au
Joan Richardson	RMIT University, Melbourne, Australia	joan.richardson@rmit.edu.au

* Corresponding author

ABSTRACT

Aim/Purpose	Inconsistent findings on the effect of various determinants of cyber security behaviour emphasise the need for further understanding of the applicability of compliance theories. The paper provides a critical review of determinants of users' cyber security behaviour and establishes directions for future research.
Background	Cyber security behaviour has been studied using a range of behavioural theories. Factors from these theories help organisations to develop suitable initiatives to encourage positive compliance from the employees.
Contribution	The paper integrates factors that can impact cyber security behaviour from Theory of Planned Behaviour, Protection Motivation Theory, Rational Choice Theory and General Deterrence Theory into an overarching framework for better connection of the theories. Previous studies' findings were analysed to establish research challenges in the field.
Future Research	Future research should investigate the complex interaction between organizational and personal characteristics so that a security program can be developed that can effectively engage employees with security tasks even in demanding work environment.
Keywords	security compliance, theory of planned behaviour, protection motivation theory, rational choice theory, general deterrence theory

Accepting Editor: Eli Cohen | Received: (date) | Revised: (date) | Accepted: (date).
Cite as: Pham, H-C., Brennan, L., & Richardson. J. (2017). Review of behavioural theories in security compliance and research challenges. *Proceedings of the Informing Science and Information Technology Education Conference*, *Vietnam,* pp. 65-76. Santa Rosa, CA: Informing Science Institute. Retrieved from http://www.informingscience.org/Publications/3722

INTRODUCTION

The main objective of information security is to protect confidentiality, integrity and the availability of respective data, information and organisational computer services (Dhillon & Backhouse, 2001). Information security is the practice of defending the safety of data and information in a computer system against unauthorised disclosure, modification, or destruction. In addition, information security also protects the computer system itself and resources against unauthorised use, modification, or denial of service (von Solms & von Solms, 2004). Traditionally, information security measures were designed to address security risks in four phases: deterrence, prevention, detection, and recovery (Warkentin & Willison, 2009). The deterrence and prevention phases aim to discourage and minimise breaches of individuals located within or outside the organisation from intentionally or accidentally violating security policies or procedures, which may lead to compromises of confidentiality, integrity, or availability of information and computing resources. The detection and recovery phases aim to detect unauthorised security activities and recover damaged information or systems and restore them to their original conditions prior to the security violation.

Users' failure to follow security procedures is the most common cause of security problems rather than deliberate harmful external attack events (Crossler et al., 2013). Various organisational and personal factors can influence how employees respond to security requirements (Furnell & Rajendran, 2012). With the advancement of security technologies, certain measures can be automated and therefore little user involvement is required, thus reducing the potential for human errors while ensuring information security objectives. For some security measures or practices that cannot be fully automated, however, user compliance is vital to ensure effective security management. Security compliance describes the behaviour of users, who, for whatever reason may or may not follow an organisation's security policies when accessing corporate IT networks and services (Warkentin & Willison, 2009). Security measures are less effective if the employees do not use them and choose to act unsafely. For example, automatically scheduled password changes together with password complexity checks can minimise reliance on users to regularly update and use difficult-to-guess passwords. Hence, users may change passwords repeatedly and have to create difficult-to-guess ones. However, some users may resort to writing down passwords on a sticky note and attaching the note to their computer for easy access. These types of unsafe practices can defeat even the most sophisticated security systems.

Security compliance as an individual behavioural choice can be affected by organisational and personal factors. Several behavioural theories have been employed as the underpinning framework in compliance studies. For example, Theory of Planned Behaviour (TPB) (Ajzen, 1991), Protection Motivation Theory (PMT) (Rogers, 1983), General Deterrence Theory (GDT) (Gibbs, 1975), and Rational Choice Theory (RCT) (Becker, 1968) have been examined in terms of their effect on security compliance intention and behaviour. Given the existence of a wide range of compliance determinants from several theories, this paper aims to organise those determinants into an overarching framework based on the TPB and highlight remaining challenges in motivating employees' security compliance.

The paper is structured as follows. The next section presents the TPB as an overarching framework to incorporate compliance factors from other behavioural theories. Future research directions to address remaining challenges are discussed in the third section. The final section is a brief conclusion with suggestions for future research.

REVIEW OF BEHAVIOURAL SECURITY COMPLIANCE THEORIES

Security compliance refers to the behaviour of users in accordance with security polices when accessing and using the IT network and services. Thus, behavioural theories have been used widely in security compliance literature to understand factors that motivate user security compliance (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). The TPB is one of the most influential frameworks for

studying human behaviour, as it explains behavioural antecedents (Ajzen, 2001). The TPB states that perceived behaviour control, attitude towards the behaviour, and subjective norms which predict intention account for a considerable amount of actual behaviour. For example, the TPB predicts that a customer may have an intention to buy a car if he/she knows how to drive it, whether he/she has a positive impression of some aspects of the car, and favourable feedback received from acquaintances that have purchased the same or a similar vehicle. A strong purchase intention towards the car is a strong indication that the customer will buy it.

Perceived behavioural control refers to evaluation of factors, whether internal or external, that facilitate or impede the performance of the behaviour (Ajzen, 2002). User attitudes towards behaviour can include positive or negative personal evaluation of performing (or not performing) a behaviour. Subjective norms are beliefs about other people's expectations about the behaviour that results in perceived social pressure to perform (or not to perform).

In other words, the TPB clearly distinguishes three different stages leading to behaviour. In stage one various factors can influence the attitude towards a behaviour. In stage two, behavioural controls, attitudes, and subjective norms influence an intention towards performing the behaviour, and lastly the intention significantly predicts the actual behaviour (Ajzen 2001). The relationship between behavioural factors influencing potential security compliance is described in Figure 1.

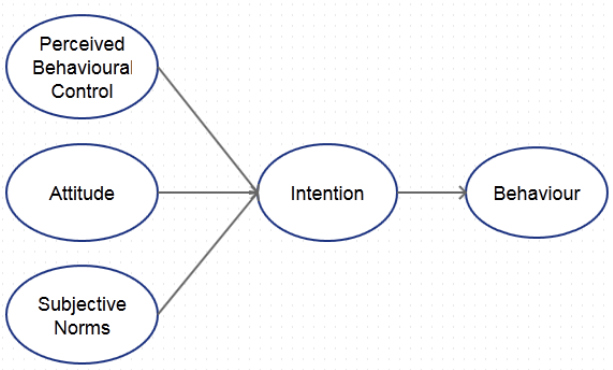

Figure 1. Theory of Planned Behaviour (Adapted from Ajzen, 2001)

In the context of security compliance, the TPB posits that if an employee (1) perceives sufficient capacity to complete the security task, (2) enjoys a favourable attitude towards performing it, and (3) observes other people in the organisation are also actively performing the practice, he/she will likely comply, which can result in actual security compliance. Studies in behavioural security compliance have explored antecedents of compliance attitudes, intention, and behaviour (Sommestad et al., 2014).

In accordance with the TPB's main argument on relationship between intention and behaviour, most studies on security compliance measured security intention as the dependent construct and argued that intention would lead to actual behaviour (Sommestad et al., 2014). A main reason that most studies stopped short of recording actual security behaviour is that monitoring the behaviour in an organisation is difficult (Crossler et al., 2013). For instance, security behaviour can be recorded indirectly through electronic means, such as server logs, cameras, or through managerial monitoring of user behaviour. However, access to accurate security information sources detailing user security actions in organisational contexts can be difficult to obtain for research purposes due to cost and confidentiality concerns (Warkentin, Straubb, & Malimagea, 2012).

The following sections present factors from GDT, RCT and PMT that may predict security intention to comply using the TPB as the underpinning framework.

Perceived Behavioural Control

Perceived behavioural control refers to the perceived ease or difficulty of performing the security compliance requirements, which can depend on whether a person may, or may not, have the ability to perform the intended tasks. Perceived behavioural control can impact a person's beliefs about their intentions and actions (Ajzen, 2002). The concept of self-efficacy is described using Bandura's (1977) Social Cognitive Theory, and Icek Ajzen's (1991) TPB as a component of perceived behavioural control (Maddux & Volkmann, 2010). The control construct describes one's self-confidence in one's ability to mobilise motivation, cognitive resources, and actions needed to successfully complete a specific task within a given context. Self-efficacy influences the amount of effort, initiation, and maintenance of coping efforts in adverse situations (Bandura, 1997).

Security self-efficacy describes individuals' security knowledge and expertise that enables them to perform their security tasks, as well as cope with changing security requirements. Self-efficacy is also included in PMT, which theorises that knowledgeable and skilful employees are more amenable to take protective security tasks (Vance, Siponen, & Pahnila, 2012). Self-efficacy has been recognised as a key factor that positively influences security compliance (Rhee, Kim, & Ryu, 2009; Johnston & Warkentin, 2010). For example, self-efficacy was reported to have a positive impact on protection motivation and related compliance with security policies (Vance et al., 2012), to strengthen security effort (Rhee et al., 2009), and directly influence individual security practice (Rhee et al., 2009; Vance & Siponen, 2012).

Another component of perceived behavioural control is locus of control, which is the perception of whether a person can control the outcome of their behaviour due to either internal or external factors (Ajzen, 2002). Self-efficacy is often considered as an internal locus of control, while the external control in security compliance refers to organisational factors that may affect an employee's capacity to perform security tasks (Cox, 2012). For example, employees need organisational resources, such as time to get acquainted with security policies, or easy access to the policies, or training required in order to comply with security policies (Pahnila, Siponen, & Mahmood, 2007). External locus of control was not consistently found to positively affect compliance intentions. Cox (2012) noticed that organisational supports did not contribute to perceived behavioural control or compliance intention. Pahnila et al. (2007) reported compliance facilitating conditions negatively affected compliance intention and argued that users viewed external security processes as the responsibilities of the organisation. Consequently, the more effective the security resources the more reliant employees would be on the organisation. Users often leave security responsibility to security managers and the technology.

Antecedents of Attitude towards Security Compliance

Several TPB-based studies have found that attitude towards a behaviour can be the strongest predictor of behavioural intent (Westaby, 2005). Likewise, the majority of security compliance literature has focused on investigating the compliance attitude and its antecedents to predict actual compliance (Bulgurcu, Cavusoglu, & Benbasat, 2010; Sommestad et al., 2014). Other behavioural theories have also been applied to explain how compliance attitudes can be formulated; thus appropriate measures can be used to alter user attitudes towards security compliance. Factors from three behavioural theories including PMT, GDT and RCT are now reviewed to explain how security compliance attitudes can be affected by various factors.

Severity and Vulnerability of Security Threats

PMT has been widely used to explain protective behaviour due to fear (Rogers, 1983). Individuals are motivated to protect themselves from physical, social, and psychological threats by invoking coping mechanisms, which are conducted by assessing threat and appraising relevant actions (Rogers, 1983). PMT states that fear influences cognition, attitudes, intentions, and protective actions. Threat appraisal comprises assessment of perceived severity, vulnerability, and rewards (benefits of taking a risk). Coping appraisal assessment comprises response efficacy, cost and self-efficacy, which deter-

mine how well people perceive themselves as being able to respond to a threat. Protection motivation (i.e., protective intention) is a mediating variable whose function is to evoke, sustain, and direct protective behaviour, which facilitates the adoption of adaptive behaviours (taking the advised behaviours) if the execution of the advised behaviour leads to a reduction of fear (Suton, 1982). In a situation where the performance of the advised behaviour does not lead to a reduction of fear, maladaptive coping actions, such as denial of the threat or avoidance of the fear-evoking message, may be used as a way of avoiding fear. PMT has been applied to health-related behaviours, such as reducing alcohol use (Stainback & Rogers, 1983), enhancing healthy lifestyles (Stanley & Maddux, 1986), enhancing diagnostic health behaviours (Rippetoe & Rogers, 1987), and prevention of disease (Tanner, Hunt, & Eppright, 1991).

Unsafe security behaviour can be compared to making unhealthy behavioural choices. People comply with security measures to reduce the fear of breach consequences (Crossler et al., 2013). PMT-based compliance approaches argue that when facing a security threat, an employee conducts threat and coping assessments to determine an adaptive (compliance) or maladaptive response (non-compliance) (Vance et al., 2012).

The severity of a security threat is measured by the characteristics evidencing its negative impacts on the organisation including confidentiality, integrity, and availability of access to information and resources. Perceived severity of a threat, such as the negative impact of opening an infected email attachment, will influence a user to behave more cautiously by limiting or eliminating such practice. Users are more likely to respond to security risks that are more certain than those less likely to happen (Rogers, 1983). Vulnerability or likelihood of security threats represent how likely an employee perceives that an unwanted incident will happen, if they do not complete a required security task (Vance et al., 2012). However, individuals can have different perceptions of vulnerability to the same security threat as one may perceive a security threat as very likely, while another feels quite the opposite (Ng, Kankanhalli, & Xu, 2009). Consequently, for the same security risk an employee can take a preventive measure against the risk while another may ignore it.

Response efficacy assesses the perceived effectiveness of taking security measures to minimise the risk of a security threat. The resources and security measures that the organisations provide and implement to facilitate employees' security compliance should demonstrate their effectiveness against the threats. Security measures that are perceived as more effective would influence an employee to take other recommended measures given alignment between their competence and the security system's requirements (Vance et al., 2012). Similar to the TPB the PMT also speculates that self-efficacy is a determinant of protection motivation. Self-efficacy can positively influence protective behaviour such as performing security tasks (Herath & Rao, 2009a; Ifinedo, 2011; Vance et al., 2012).

PMT-based studies found evidence for mixed impacts of threat assessments on compliance attitudes and intentions. The security threat severity and the perceived effectiveness of the measures (i.e., response efficacy) have a strong influence on the intention of taking the advised security behaviour (Vance et al., 2012). Nevertheless, Cox (2012) did not find that risk severity had a significant role in users' intention. Likewise, the impact of vulnerability on compliance intention was not clear. An insignificant impact of vulnerability on compliance intentions was observed (Vance et al., 2012), it was, however, identified as positively affecting compliance intention (Ifinedo, 2011).

Fear-based communications help promote security compliance by ensuring users are aware of the severity and vulnerability of security risks, and the effectiveness of preventative measures provided by the organisation (Brennan & Binney, 2010). When facing potential security risks, people may assess the severity of the risks and act in a way to avoid the consequences, especially if non-compliance evokes a punishment. A clearly described and understood risk that is likely to occur would be more likely to have an impact on compliance choices. Given a similar level of a security threat, a less likely threat would have less influence on the user's motivation to act safely and avoid risk.

There are some issues related to the effectiveness of using a fear-based compliance approach. Poor security communication makes it difficult for users to respond to a real security threat since they may underestimate the likelihood of the threat. Often users are motivated to respond to a security threat when the risk is evident and personal (Pfleeger & Caputo, 2011). Furthermore, little is known about the circumstances in which individuals feel fearful and the characteristics of the individuals that may serve to accentuate or diminish the emotion of fear in security compliance situations (Crossler et al., 2013). Finally, Brennan and Binney (2010) stated that externally motivated fears have a short term motivating influence and are not self-sustaining, hence they are not effective to motivate security compliance in the long term.

Response Cost for Compliance

Attitudes towards security compliance can be drawn from RCT, which puts forward two premises for the consideration of an offence (non-compliance): (1) balancing the costs and benefits of offending, and (2) the decision maker's perceived or subjective expectation of reward and cost (Becker, 1968).

For example, the habits of changing password frequently and more difficult to guess are impacted positively from the training, enforcement of acceptable use policy (AUP), monitoring, and reward system. However, the more frequently changing and the more difficult of guessing passwords, the more difficult for individuals to remember their passwords and the more likely an individual will write them down (Stanton, Stam, Mastrangelo, & Jolton, 2005). Therefore, the increase in training, AUP, monitoring, and reward systems may lead to the higher risk of losing information but very slightly. Correspondingly, the more a user perceives favourable rewards for non-compliance, the higher the chance he/she does not comply with security policies. An example of a reward for non-compliance could be saving time (Woon, Tan, & Low, 2005). When the perceived direct costs to the users incurred from the security threat are lower than the indirect cost or effort required by the user to circumvent the threat, users can ignore security compliance requirements (Schneier, 2008).

Inconsistent findings on the impacts of compliance costs on intention to comply have been reported in prior studies. Ng et al. (2009) noticed that a perceived barrier or inconvenience for practising safe email had an insignificant impact on the users' safe email practice. Security response efficacy and self-efficacy were found to have a direct and significant impact on compliance intentions, whereas response cost and security concerns did not appreciably contribute to predicting compliance intentions (Herath & Rao, 2009b).

Vance et al. (2012), however, detected that compliance cost negatively influenced employees' compliance intention due to employees considering the inconvenience of following information security policies a legitimate reason for not complying with those policies. Employees may find security compliance time-consuming and inconvenient as it has the potential to obstruct their daily routine work, which negatively impacts compliance levels (Dhillon & Torkzadeh, 2006; Vance & Siponen, 2012).

There are inconsistent findings on the impact of compliance cost on security behaviour. Contextual factors such as organisational support and personal resources may affect the impact of personal response cost on compliance intention (Herath & Rao, 2009a).

Sanctions for Non-Compliance and Rewards for Compliance

GDT has been used as a theoretical basis for understanding why employees follow (or do not follow) their organisation's information security policies (Hu, Xu, Dinev, & Ling, 2011). GDT emphasises the use of punishments to deter people from offending, which proposes that individuals assess deterrent certainty and severity to determine actions to be taken when a violation of the rules occurs (Gibbs, 1975). In a security compliance context, organisations might employ security mandates and disciplinary actions to manage and motivate compliance (Bulgurcu et al., 2010; Herath & Rao, 2009a).

As a result, communications of certainty and severity of penalties for rule-breaking behaviour have been considered to be effective strategies in preventing employees from violating security policies.

GDT-based security measures are mainly based on fear of punishment as an antecedent to changing an undesirable behaviour. However, the effectiveness of threats of punishment to achieve security compliance has been inconsistent. For example, fear of penalties for non-compliance has been reported to have a significant impact on security behaviour (Herath & Rao, 2009a). These studies showed that if employees perceive high certainties of being caught for violating security policies, they were more likely to comply; moreover, the certainty of being detected outweighs fear of the punishment's severity. On the contrary, other studies found that sanctions did not have a significant impact on actual compliance (Herath & Rao, 2009a; Hu et al., 2011).

Associated with sanctions for non-compliance, rewards can also be used to promote compliance. Rewards can include tangible or intangible compensations that an organisation gives to an employee in return for compliance with the security requirements. Compensations may include monetary rewards, such as pay rises or bonuses, or nonmonetary rewards, including personal mention, formal recognition in oral or written assessment reports, and promotions (Bulgurcu et al., 2010).

The granting of rewards for security compliance may not yet be common practice (Guo & Yuan, 2012). Boss, Kirsch, Angermeier, Shingler, and Boss (2009) argued that rewards may increase how mandatory users perceive compliance with security policies, which in turn may enforce security precaution-taking behaviour. Similarly, Pahnila et al. (2007) and Siponen, Mahmood, and Pahnila (2014) hypothesised that rewards would increase actual security compliance. Both studies, however, found rewards did not contribute to either how obligatory security compliance was perceived to be (Boss et al., 2009) or actual compliance (Pahnila et al., 2007).

Reasons that may explain the inconsistent findings of the effectiveness of sanctions and lack of support for rewards in motivating security compliance are:

- Few organisations implement schemes of sanctions and rewards for security compliance, so the actual effectiveness cannot be measured. In addition enforcing a sanction and reward-based approach can have a negative impact on staff cooperation(Guo & Yuan, 2012).
- Boss et al. (2009) explained that, unlike other work tasks, there is little that an individual can do to exceed expected security compliance; hence organisations may not employ compliance rewards.
- Penalising or rewarding a user can be impractical for organisations due to time constraints and difficulty in the description of a concrete evidence trail (Guo & Yuan, 2012).
- Promoting compliance through sanctions could promote a culture of lies, deception, and avoidance of responsibility (Ramachandran, Rao, & Goles, 2008).

Subjective Norms

The impact of social influences on an individual's behaviours and beliefs have been widely acknowledged (Cialdini & Goldstein, 2004). Social influences are often referred to as subjective norms (Ajzen, 1991) and can take the form of introjected motivation (Gagné & Deci, 2005). For instance, subjective norms refer to the users' beliefs about the normative expectations and social pressure that drive people's intention to perform security behaviours, as posited in the TPB (Ajzen, 1991). Self-motivation for security compliance is the ideal where people can be trusted to work within relevant parameters without surveillance, thereby decreasing costs of security monitoring. In the absence of self-motivation, extrinsic factors and other people (social influences and relatedness) can motivate people to comply with security requirements. Members of a work environment, such as peers, colleagues, or supervisors, can exert social influence on an individual to perform security tasks (Johnston & Warkentin, 2010). If an employee believes that other important members in the workplace expect security compliance from him/her, then he/she is more likely to perform appropriate security tasks (Bulgurcu et al., 2010). Subjective norms are sometimes also referred to as social influence (Johnston & Warkentin, 2010) or normative beliefs (Bulgurcu et al., 2010). The positive effect of subjective norms on compliance intention has been reported in several studies (Bulgurcu et al., 2010; Vance et al., 2012).

RESEARCH CHALLENGES FOR IMPROVING SECURITY BEHAVIOUR

Based on the review of the behavioural compliance theories above, several research challenges are now presented in Table 1.

Table 1. Summary of Behavioural Security Theories based on TPB

Behavioural Theory	Factors	Challenges
TPB – Perceived Behaviour Control	1. Key factors: self-efficacy to perform security tasks, attitudes toward compliance and security practice of other stakeholders. 2. Security compliance can be enhanced by developing self-efficacy, creating a positive attitude toward security tasks, and establishing an organisational safe security culture.	a. A main assumption that compliance intention would lead to security behaviour. b. May not accurately capture determinants of actual security behaviour. c. Need to employ methods of recording true security behaviour and less reliant on self-reported responses.
TPB – Attitude Protection Motivation Theory	1. Factors: fear of consequences of security threats, effectiveness of response measures 2. Security compliance can be encouraged by communicating security risk severity and vulnerability, effectiveness of security measures, and training to enhance self-efficacy.	a. Focusing on nature of security risks. b. Accurate risk assessment is difficult due to its complexity and subject to behavioural biases, which affect individuals' ability to assess a risk objectively and accurately. c. Short-term effectiveness in changing security behaviour.
TPB – Attitude General Deterrence Theory	1. Key factors: fear of severity and likelihood of sanctions for non-compliance. 2. Security compliance can be achieved employing strict security behaviour monitoring and implementation of disciplinary actions.	a. Focusing external enforcement measures. b. Costly security monitoring can have negative impact on staff morale and cooperation.
TPB – Attitude Rational Choice Theory	1. Key factors: perceived extrinsic cost and benefits of performing security tasks. 2. Security compliance can be motivated by streamlining security processes, minimising impacts of security tasks on work productivity, and providing resources to facilitate users' compliance.	a. Security compliance cost may be unavoidable. Lack of immediate benefits of compliance. b. Lack of understanding of characteristics of security tasks and compliance cost. c. Low compliance cost still does not guarantee better compliance.

While existing studies employing numerous behavioural theories provide a solid foundation for explaining employees' security compliance decisions, a complete knowledge of the phenomenon remains a challenge. Evidence of the incomplete knowledge can be shown in the percentage of explained variance of the compliance variable outcome in existing security compliance models, which varies between 25-70 per cent range (Sommestad et al., 2014). A complete understanding of security behaviour is problematic because it can be affected by many environmental and personal factors. Furnell and Rajendran (2012) identified a mix of job characteristics, and organisational and non-work factors that all play a role in affecting employees' security compliance. To complicate the issue fur-

ther, individuals' personality attributes can also act as a filter of the environmental impact and affect individual attitudes and behaviour toward security behaviour (Furnell Rajendran, 2012; Pfleeger & Caputo, 2011).

CONCLUSION

Employees' unsafe security behaviour has been considered the weakest link in overall security programs. Safe security practice and complying with security guidelines are essential to minimise security risks caused by the users. Current behavioural theories have contributed to better understanding of how security behaviour can be improved, though not yet complete. This paper reviews key factors influencing security compliance based on several behavioural theories. Challenges to successfully apply those factors are identified and future research is proposed. The paper recommends that combined organisational and personal focuses which embolden employees to become involved with security activities is important; nevertheless, the level of emotional and cognitive resources that people bring to performing security tasks might be the key to maintenance of expected security behaviour, even in an unfavourable security environment (Crawford, LePine, & Rich, 2010).

Future research should investigate the complex interaction between organizational and personal characteristics so that a security program can be developed that can effectively engage employees with security tasks even in demanding work environment.

REFERENCES

Ajzen, I. (1991). Theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. doi:10.1016/0749-5978(91)90020-T

Ajzen, I. (2001). Nature and operation of attitudes. *Annual Review of Psychology, 52*(1), 27-58.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology, 32*(4), 665-683.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215. doi: http://dx.doi.org/10.1037/0033-295X.84.2.191

Bandura, A. (1997). *Self-efficacy: The exercise of control*. New York: Freeman.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*(2), 169.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*, 151-164.

Brennan, L., & Binney, W. (2010). Fear, guilt and shame appeals in social marketing. *Journal of Business Research, 63*(2), 140-146.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology, 55*, 591–621. doi: 10.1146/annurev.psych.55.090902.142015

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*, 1849-1858.

Crawford, E. R., LePine, J. A., & Rich, B. L. (2010). Linking job demands and resources to employee engagement and burnout: A theoretical extension and meta-analytic test. *Journal of Applied Psychology, 95*(5), 834-848. doi: http://dx.doi.org/10.1037/a0019364

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hud, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computer & Security, 32*, 90-101. doi: 10.1016/j.cose.2012.09.010

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems, 11*, 127-153.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems, 16*(3), 293-314.

Furnell, S., & Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security, 2012*(3), 12-15. doi: 10.1016/s1361-3723(12)70053-2

Gagné, M., & Deci, E. L. (2005). Self-determination theory and work motivation. *Journal of Organizational Behavior, 26*, 331-362.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York, NY: Elsevier.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*, 320-326.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*, 154-165. doi: 10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*, 106-125. doi: 10.1057/ejis.2009.6

Hu, Q., Xu, Z. C., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

Ifinedo, P. (2011). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*, 83-95. doi: 10.1016/j.cose.2011.10.007

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *Management Information Systems Quarterly, 34*(3), 549-566.

Maddux, J. E., & Volkmann, J. (2010). *Self-efficacy handbook of personality and self-regulation*: Blackwell Publishing Ltd.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 4*, 815-825.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' Behavior towards IS security policy compliance*. Paper presented at the 40th Hawaii International Conference on System Sciences.

Pfleeger, S. L., & Caputo, D. D. (2011). Leveraging behavioral science to mitigate cyber security risk. *Computer & Security, 31*, 597-611.

Ramachandran, S., Rao, S. V., & Goles, T. (2008). *Information security cultures of four professions: A comparative study*. Paper presented at the 41st Hawaii International Conference on System Sciences.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computer & Security, 28*, 816-826.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology, 52*, 596-604.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology*: New York: Guilford Press.

Schneier, B. (2008). *The psychology of security*. Retrieved from http://www.schneier.com/essay-155.html

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employee's adherence to information security policies: An exploratory field study. *Information & Management, 51*, 217-224. doi: 10.1016/j.im.2013.08.006

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security, 22*(1), 42–75. doi: http://dx.doi.org/10.1108/IMCS-08-2012-0045

Stainback, R. D., & Rogers, R. W. (1983). Identifying effective components of alcohol abuse prevention programs: Effects of fear appeals, message style and source expertise. *International Journal of Addictions, 18*, 393-405.

Stanley, M. A., & Maddux, J. E. (1986). Cognitive processes in health enhancement: Investigation of a combined protection motivation and self-efficacy model. *Basic and Applied Social Psychology, 7*, 101-113.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computer & Security, 24*, 124-133.

Suton, S. R. (1982). Fear-arousing communications: a critical examination of theory and research. In J.R Eiser (Ed.), *Social psychology and behavioural medicine* (pp. 303-337). London: Wiley.

Tanner, J. F. J., Hunt, J. B., & Eppright, D. R. (1991). The Protection Motivation Model: A normative model of fear appeals. *Journal of Marketing, 55*(July), 36-45.

Vance, A., & Siponen, M. (2012). IS Security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing, 24*(1), 21-41. doi: 10.4018/joeuc.2012010102

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*, 190-198. doi: 10.1016/j.im.2012.04.002

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computer & Security, 23*, 275-279.

Warkentin, M., Straubb, D., & Malimagea, K. (2012).-*Measuring secure behavior: A research commentary.* Paper presented at the Annual Symposium on Information Assurance & Secure Knowledge Management, Albany, NY.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*, 101-105. doi: 10.1057/ejis.2009.12

Westaby, J. D. (2005). Behavioral reasoning theory: Identifying new linkages underlying intentions and behavior. *Organizational Behavior and Human Decision Processes, 98*(2), 97-120. doi: http://dx.doi.org/10.1016/j.obhdp.2005.07.003

Woon, I., Tan, G., & Low, R. (2005). *A protection motivation theory approach to home wireless security*. Paper presented at the International Conference on Information Systems (ICIS).

BIOGRAPHIES

Dr Hiep Pham is a Senior Lecturer in the school of Business Information Technology and Logistics at the RMIT University Vietnam. He holds a PhD and EMBA from RMIT University and a Master of Commerce in Advanced Information Systems and Management from University of New South Wales, Australia. Pham's research focuses on cyber security behaviour and management, information management in Logistics & SCM and educational technologies.

Linda Brennan was the Inaugural Professor of Advertising at RMIT University. In the lead up to becoming a full time academic Professor Brennan had an active consulting practice in marketing and strategic research, working with a variety of markets, projects and industries. She has expertise on both qualitative and quantitative research methods and she has taught research strategies, research methods and 'market' research for over 10 years. She has published articles and book chapters on research methodologies (qual and quant) and has a solid understanding of paradigms, research philosophies, multi-disciplinary and interdisciplinary re-

search approaches. She is the Editor of Communication, Politics & Culture and Associate Editor for the Journal of Marketing for Higher Education as well as on the review board of several ranked journals. She has served on ethics committees in four universities and is a Research Integrity Advisor at RMIT University. She has supervised, examined and advised many PhD and Masters by Research over the last 15 years.

Joan Richardson is an Associate Professor in the Department of Business Information Technology and Logistics at RMIT University, Australia. She won an ALTC citation (2011) that recognized her particular contribution to improving student satisfaction and student engagement through the use of emerging technologies in Digital Literacy curriculum. In addition, she has worked extensively with Pearson Education Australia as the principal author for texts, e-texts and multi-media resource libraries since 2000. Innovations include the use of social networking features to enable peer engagement, SMS to disseminate assessment reminders and performance feedback, websites, multi-choice tests and communications sent from the learning management systems to personal mobile devices. Her substantial record of Information Systems (IS) research also includes six PhD completions and more than 75 peer reviewed book chapters, journals and conference publications. She presents her research publications and professional achievements, such as accreditation documentation addressing the Skills for the Information Age (SFIA) framework at national and international conferences.